UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,257	12/29/2000	Keen W. Chan	42390P10447	8790

8791 7590 03/08/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 03/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/753,257	CHAN ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24,26-31,33-44 and 46-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24,26-31,33-44 and 46-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 October 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the previous office action, Applicant has amended claims 24, 27, 28, 30, 34, 35, and 43. Claims 24, 26-31, 33-44, and 46-54 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 24, 26, 28-30, 33-38, 40, 43, 46-50, and 52 are rejected under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 6,141,760 to Abadi et al. in view of U.S. Patent No. 6,826,686 to Peyravian et al. further in view of Schneier, "Applied Cryptography," 1996, pp. 165-166 and 429-431.

Regarding claims 24, 26, 30, 33, 34, 36, 37, 40, 43, 46-49, 50, and 52, Abadi discloses a method for constructing a password specific to a service (an application) by hashing the name of the service (input data) from the user (see column 3, lines 4-5), a master password (the strong password) and the user name (see abstract). The password is then submitted to the application (see column 3, lines 60-62). The system

is designed to construct passwords for all services which a user uses, including client software applications (see column 2, lines 41-56).

Abadi does not explicitly describe the use of a random salt in password creation.

Peyravian discloses the integration of a client-specific and a server-specific random number hashed with a user_id and master user password (see column 4, lines 32-57), and suggests that this allows for password agreement without the need for a key pair or agreed-upon key while preventing replay attacks (see column 2, line 66 to column 3, line 10).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Abadi by integrating a client-specific and a server-specific random number hashed with a user_id and master user password, as disclosed by Peyravian, as this allows for password agreement without the need for a key pair or agreed-upon key while preventing replay attacks.

Abadi also does not disclose passwords that are only valid for a specified time period.

Peyravian further discloses the use of time-out mechanisms to maintain the secrecy of passwords (see column 4, lines 21-24).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the invention of Abadi by incorporating a time-out mechanism, as disclosed by Peyravian, to maintain the secrecy of passwords.

Using Abadi in view of Peyravian, a user would only need to remember the master password.

Abadi and Peyravian only disclose the computing of the hash a single time.

Schneier discloses an algorithm for iteratively hashing a value any number of times (see "Length of One-Way Hash Functions," pp.430-431), and notes that additional hashing increases resistance to birthday attacks (see pp. 429-430; a description of birthday attacks in found on pp. 165-166).

Therefore it would been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Abadi and Peyravian by hashing a value multiple times, as disclosed by Schneier, to increase resistance to birthday attacks.

As per claims 28 and 35, a single master password is used to create multiple application passwords.

Regarding claims 29, the incorporation of a server-specific random number, the salt value is unique to each application.

Regarding claims 34, 47, and 48, Abadi does not disclose a mechanism for changing passwords if it is determined that a change is necessary.

Peyravian discloses a mechanism for changing passwords if the master password is changed (due to a time-out, for example), because the password may have been discovered by someone else (see whole document, especially column 4, lines 21-31).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Abadi by supplying a mechanism to change passwords is the master password needs changing, as disclosed by Peyvarian, because the password may have been discovered by someone else.

As per claim 38, a networked system is used (see Abadi, column 2, lines 21-23).

3. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,141,760 to Abadi et al. in view of U.S. Patent No. 6,826,686 to Peyravian et al. in view of Schneier, "Applied Cryptography," 1996, pp. 165-166 and 429-431 as applied to claim 24 above, and further in view of U.S. Patent No. 5,719,941 to Swift et al.

Abadi, Peyravian, and Schneier do not disclose the use of the old password in the method.

Swift discloses the use of the generated old password in the forming of the encryption/decryption key (see abstract), and further suggests that this ensures that the source of the new password is authorized to change the password (see column 3, lines 26-31).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Abadi, Peyravian, and Schneier by using the old password in the password updating algorithm, as disclosed by Swift, as this ensures that the source of the new password is authorized to change the password.

4. Claims 31 and 44 are rejected under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 6,141,760 to Abadi et al. in view of U.S. Patent No. 6,826,686 to Peyravian et al. in view of Schneier, "Applied Cryptography," 1996, pp. 165-166 and 429-431 as

applied to claims 30 and 43 above and further in view of U.S. Patent No. 6,006,333 to Nielsen.

Over and above what is described and Abadi, Peyravian, and Schneier above, Abadi discloses the generation of user names for storage in a set of user names (203), which is then retrieved to generate the password (see column 3, lines 22-45).

Abadi, Peyravian, and Schneier do not specifically disclose a test to see if the user name already exists.

Nielsen discloses a system for maintain passwords for different applications wherein there is a check to see if a password exists, and an entry may be created if none exists. This is done to allow the user to register at the new site (see column 5, lines 40-61).

Therefore it would be obvious to one of ordinary skill in the art to modify the invention of Abadi, Peyravian, and Schneier by checking to see if a password exists, and an create an entry if none exists, as disclosed by Nielsen, in order to allow the user to register at the new site.

5. Claims 39 and 51 are rejected under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 6,141,760 to Abadi et al. in view of U.S. Patent No. 6,826,686 to Peyravian et al. in view of Schneier, "Applied Cryptography," 1996, pp. 165-166 and 429-431 as applied to claims 30 and 43 above and further in view of U.S. Patent No. 6,064,736 to Davis et al.

Abadi, Peyravian, and Schneier do not disclose the algorithm to be used in the construction of the hash.

Davis discloses the use of the MD5 algorithm for constructing a password hash, and suggests that this allows a server to transport information safely to a client (see column 3, lines 56-65).

Therefore it would be obvious to one of ordinary skill in the art to modify the invention of Abadi, Peyravian, and Schneier by using the MD5 algorithm for constructing the password hash, as disclosed by Davis, as this allows a server to transport information safely to a client.

6. Claims 41, 42, 53, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,141,760 to Abadi et al. in view of U.S. Patent No. 6,826,686 to Peyravian et al. in view of Schneier, "Applied Cryptography," 1996, pp. 165-166 and 429-431 as applied to claims 30 and 43 above, and further in view of U.S. Patent No. 6,601,175 to Arnold et al.

Abadi in view of Peyravian does not provide for a password that is only valid for a limited time period based on platform activity.

Arnold discloses the derivation of limited-time passwords for local computer use or remote administration, which can be created on an as-needed basis (based on platform activity), and further suggests that this is done to prevent a user from re-configuring a computer after learning the administrative password (see column 5, lines 10-44).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention disclosed by Abadi, Peyravian, and Schneier by supporting limited-time passwords, as disclosed by Arnold, to prevent a user from re-configuring a computer after learning the administrative password.

Response to Arguments

7. Applicant's arguments, see Remarks, filed 19 December 2005, with respect to the rejections of the claims under 35 U.S.C. 103 have been fully considered and are persuasive in view of Applicant's amendments. Therefore, the rejection has been withdrawn. However, upon further consideration, new grounds of rejection are made in view of the previously cited art in view of Schneier.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu, can be reached at (571) 272-3859.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

February 22, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100